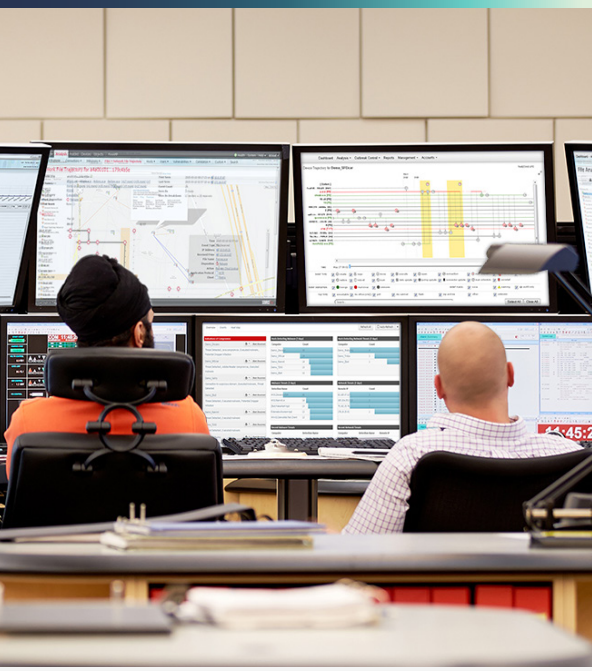
At-A-Glance



Cisco Advanced Malware Protection for Endpoints

メリット

- マルウェアの**継続的な検出と監視**を迅速かつ遡及的に実施
- **Windows オペレーティング システム**、Mac、Linux、およびモバイル デバイスの保護
- マルウェアの拡散を追跡し、侵害の範囲を特定するための長期的な**ファイル活動の記録**
- **異なるイベント**を一連の攻撃に関連づけ
- **ネットワーク防御を強化する**グローバル脅威情報へのアクセス
- **侵害をすばやく検出、分析、修復するための**高度な可視性、コンテキスト、および制御
- **エージェントレス検出機能**により OS レベルでの侵害が発生する前にマルウェアを捕捉

現実社会におけるセキュリティ侵害の防御、検出、対応、および修復

ハッカーは、ウィルス対策や侵入防御システムなど、最強の防止ツールでさえすり抜ける高度なマルウェアを作成しています。これらのツールは、すべての脅威を防止する点で 100 % 有効ではありません。また、最初の防御をすり抜けた脅威の活動を可視化することもできません。この結果、IT セキュリティ チームは潜在的な危害の範囲を認識することができず、損害を与える前にすばやくマルウェアを検出および修復することができないのです。

Cisco AMP for Endpoints は、クラウド管理エンドポイント セキュリティ ソリューションであり、侵害を防止するため、および最前線の防御をすり抜けた脅威が損害を引き起こす前にこのような脅威を迅速に検出、封じ込め、修復するために必要な可視性、コンテキスト、および制御機能を備えています。また、コスト効率に優れ、運用効率に悪影響を与えることはありません。

- **防止**：最良のグローバル脅威インテリジェンスを使用して防御機能を強化し、マルウェアをリアルタイムでブロックします。
- **監視および検出**：すべてのファイル アクティビティを継続的に監視、記録し、隠されたマルウェアを迅速に検出します。
- **対応**：PC、Mac、Linux、モバイル デバイスを対象に、調査にかかる時間を短縮し、マルウェアを自動的に修復します。

脅威インテリジェンスおよび動的マルウェア分析

Cisco AMP は、Talos Security Intelligence and Research Group および Threat Grid インテリジェンス フィードから提供される、リアルタイムの脅威インテリジェンスと動的マルウェア分析の広範なコレクションをベースに構築されています。

組織にとってのメリット：

- 150 万件の着信マルウェアのサンプル（1 日あたり）
- 160 万個のグローバル センサー
- 1 日で 100 テラバイトのデータ
- 130 億件の Web 要求
- エンジニア、技術者、および研究者のチーム
- 24 時間運用

機能

継続的な分析およびレトロスペクティブ セキュリティ：AMP は、ファイル アクティビティを継続的に監視、分析、記録し、最前線の防御をすり抜けるマルウェアを迅速に検出します。これは、侵害の範囲を特定して、迅速に対応するのに役立ちます。

動的なマルウェア分析とサンドボックス：広範な動作指標を使用してマルウェアを分析し、以前は不明だったゼロデイ脅威を発見できます。

侵入の痕跡（IoC）：ファイル、テレメトリ、および侵入イベントが相関付けられ、アクティブな侵害の可能性があるものとして優先度が設定されます。これにより、セキュリティ チームはマルウェア インシデントを迅速に特定し、より大規模な組織的攻撃に結び付けることができます。

デバイス トラジェクトリ：デバイス上およびシステム レベルでの実行ファイルのアクティビティや通信を継続的に追跡することで、根本原因をすみやかに把握し、セキュリティ侵害の前後のイベント履歴を把握できます。

拡散度：AMP は、組織全体で実行されている拡散度の低いファイルを表示します。これは、少数のユーザのみが確認した、以前は検出されていなかった脅威を表面化させるのに役立ちます。

脆弱性：脆弱なソフトウェアを特定し、攻撃パスを遮断します。AMP は、標的にされている脆弱性のあるソフトウェアと、悪用の可能性があるものを特定し、パッチを適用するホストの一覧を優先度とともに表示します。

Cognitive Threat Analytics（CTA）との統合：平均 30 % 以上の感染を確認し、ファイルレスまたはメモリ専用マルウェアを検出し、マルウェアが OS レベルでセキュリティを侵害する前にマルウェアを捕捉し、AMP for Endpoints コネクタがインストールされていないデバイスを可視化します。

組み込みウイルス対策エンジン：ルートキット スキャン、ローカル IOC スキャン、デバイス フロー モニタリングを使用して、シグニチャ ベースの検出を実行します。シグニチャベースの AV および高度なエンドポイント保護機能を 1 つのエージェントに統合する必要があるお客様は、このエンジンを有効にして利用できます。

アウトブレイク制御：コンテンツの更新を待つことなく、脅威の拡大を制御し、修復できます。

- すべてのシステムまたは選択したシステムで特定のファイルを迅速にブロックする
- ポリモーフィック型マルウェアのファミリをブロックする
- マルウェア ゲートウェイとして使用されている侵害を受けたアプリケーションを阻止し、再感染サイクルを止める
- 企業ネットワーク外のリモート エンドポイントでも、マルウェアのコールバック通信をソースで停止する

他の機能については、AMP for Endpoints のデータシートを参照してください。

Threat Grid による AMP for Endpoints 組み込みサンドボックス技術は、毎月数百万のサンプルを 700 を超える動作指標と照らし合わせて分析します。その結果、セキュリティ チームが隠れたマルウェアを検出し、対応の優先度を設定するのに役立つ、数十億のアーチファクトや理解しやすい脅威スコアが生成されます。

継続的な分析とレトロスペクティブ セキュリティ

Cisco AMP for Endpoints は、初期検査の後も、すべてのファイルと実行可能なアクティビティを、その性質に関係なく継続的に監視、分析、記録します。AMP が疑わしいアクティビティを発見すると、セキュリティ チームにアラートが送信されます。セキュリティ チームは、脅威の完全な履歴を確認して、次の質問に対する答えを迅速に得ることができます。

- マルウェアの発生源はどこか
- 攻撃はどのような方法で行われ、どこから侵入したのか
- どこにあったかどのシステムが侵害を受けたか
- 脅威は過去および現在にどのような活動を行っているか
- 脅威を阻止して根本原因を除去するにはどうすればよいか

AMP のブラウザベースの管理コンソールでの数回のクリック操作だけで、ファイルがすべてのエンドポイントで実行されるのをブロックできます。Cisco AMP は過去にファイルが通過した他のすべてのエンドポイントを把握しているため、ファイルをすべてのユーザから隔離することができます。マルウェアを排除するために、従来のようにセキュリティ チームがシステム全体を再イメージする必要はもはやありません。その方法には多大な時間、コスト、リソースがかかっていました。AMP では、マルウェアのみを対象にピンポイントで修復を行うことができるため、IT システムやビジネスに付随的な損害が生じることはありません。

また AMP は、脅威の署名からファイルの動作まで、確認した内容をすべて記憶しており、そのデータを AMP の脅威インテリジェンス データベースに記録します。これにより第一防衛線がさらに強化されるため、そのファイル（および類似ファイル）は初期検出を回避できなくなります。

導入

Cisco AMP for Endpoints は、使いやすい Web ベースのコンソールを使用して管理します。AMP の軽量エンドポイント コネクタを使用して導入されるため、ユーザのパフォーマンスには影響ありません。分析はエンドポイントではなくクラウドで行われます。このソリューションは、Windows、Mac、Linux、モバイル デバイスなど、エンドポイントでのサブスクリプションとして提供されます。Cisco AMP for Endpoints は、AnyConnect v4.1 からも起動できます。

次のステップ

高度なサイバー攻撃から組織を保護するのに Cisco AMP for Endpoints がどのように役立つかについては、シスコの営業担当者またはチャネル パートナーにお問い合わせください。詳細については、www.cisco.com/jp/go/ampendpoint を参照してください。

C45-731874-08 02/17